STAFF SUMMARY SHEET

	TO	ACTION	SIGNATURE (Surname), GRADE AND DATE		TO	ACTION	SIGNATURE (Surname), GRADE AND DATE
1	DFER	approve	SoLTI, AD-22, 10 Jan 14	6			
2	DFMS	action		7			
3				8			
4				9			
5				10			

SURNAME OF ACTION OFFICER AND GRADE	SYMBOL	PHONE	TYPIST'S INITIALS	SUSPENSE DATE
Beth E Schaubroeck, PhD, Civ	DFMS	333-2147	bes	

SUBJECT	DATE
Clearance for Material for Public Release USAFA-DF-PA- 06	20131217

SUMMARY

1. PURPOSE. To provide security and policy review on the document at Tab 1 prior to release to the public.

2. BACKGROUND.
Authors: Michael Brilleslyper and Beth E. Schaubroeck (DFMS)

Title: Locating Unimodular Roots

Circle one: Abstract Tech Report (Journal Article) Speech Paper Presentation Poster
Thesis/Dissertation Book Other: _____

Check all that apply (For Communications Purposes):
[] CRADA (Cooperative Research and Development Agreement) exists
[] Photo/ Video Opportunities [] STEM-outreach Related [] New Invention/ Discovery/ Patent

Description: The journal article is being submitted for publication in Mathematics Magazine, a journal of the Mathematical Association of America.

Release Information: Article to be submitted to Math Horizons
Previous Clearance information: N/A
Recommended Distribution Statement: (Distribution A, Approved for public release, distribution unlimited.)

3. DISCUSSION. N/A

4. VIEWS OF OTHERS. N/A

5. RECOMMENDATION. Approve document for public release. Suitability is based solely on the document being unclassified, not jeopardizing DoD interests, and accurately portraying official policy.

JOHN M. ANDREW, Col, USAF
Chair, Basic Sciences Division
Permanent Professor and Head
Department of Mathematical Sciences

1 Tab
1. Copy of article

Locating Unimodular Roots

Introduction

The well-known formula of de Moivre ([4], pg. 22), implies the polynomial $q(z) = z^7 - 1$ has seven roots symmetrically distributed on the unit circle with one at $z = 1$ and the others equally spaced at angular intervals of $2\pi/7$. In contrast, inserting a lower order term as in $p(z) = z^7 + z^5 - 1$ results in a less symmetric pattern of the roots as shown in Figures 1 and 2. Observe, however, that two of the seven roots of $p(z)$ still appear to lie on the unit circle. This is indeed the case as we shall see below.

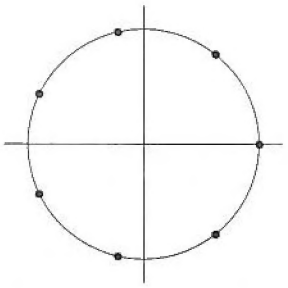

Figure 1. The unit circle and roots of $q(z) = z^7 - 1$.

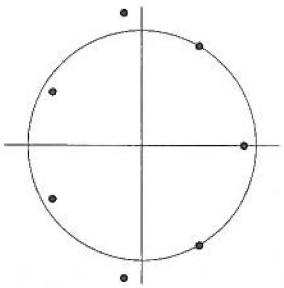

Figure 2. The unit circle and roots of $p(z) = z^7 + z^5 - 1$.

Changing the middle term of $p(z)$ from z^5 to z^4 results in the polynomial having no roots on the unit circle. Furthermore, if we consider the family of polynomial equations $z^7 + z^k - 1 = 0$ for $k = 1, 2, \ldots, 6$, then the only case in which there are solutions of unit modulus is when $k = 5$. This observation, along with other similar examples, prompted the investigations which led to this paper.

We will refer to roots that lie on the unit circle as *unimodular* roots. We ask when the polynomial $p(z) = z^n + z^k - 1$ has unimodular roots, and provide an answer in terms of conditions on n and k. Here we assume that n and k are integers with $n \geq 2$ and $1 \leq k \leq n - 1$. Throughout this paper, we let C denote the unit circle in the complex plane.

Inserting the lower order term z^k in the polynomial $q(z) = z^n - 1$ results in a complicated pattern for the location of the roots. For example, Figure 3 shows all 380 roots for the family of polynomials given by $p(z) = z^{20} + z^k - 1$, where $1 \leq k \leq 19$. It appears that some of these roots are unimodular, but most are not. We will see that when $k = 4$, eight of the twenty solutions to $z^{20} + z^4 - 1 = 0$ are unimodular, but for $k \neq 4$, there are no unimodular solutions.

For a different example, if $n = 17$, then the corresponding family of polynomials, $p(z) = z^{17} + z^k - 1$, has exactly two unimodular roots when $k = 1, 7$, or 13. For all other values of k there are none.

Studying the roots of trinomials is an old problem dating back to the nineteenth century. Melman's recent paper [2] provides improved bounds on both angular sectors and annular regions containing the roots. It also gives historical references to several of the original papers on this topic.

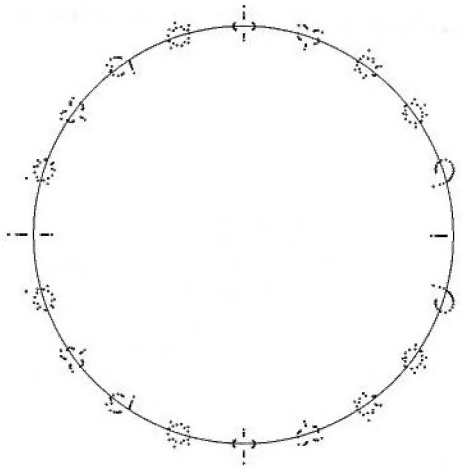

Figure 3. The unit circle and the 380 roots of $p(z) = z^{20} + z^k - 1$, for $1 \leq k \leq 19$.

More generally, the problem of counting the number roots of a polynomial that occur inside, on, or outside the unit circle has been extensively studied. The Schur-Cohn procedure (see **[3]**) provides a recursive method for counting these quantities for a given polynomial. However, the trinomials we study here are singular cases for the Schur-Cohn algorithm. There are variations of the algorithm to handle the singular cases, but they are difficult to implement and unlikely to yield an explicit formula for the number of unimodular roots in terms of n and k. Another shortcoming of the Schur-Cohn approach is that the algorithm fails to specify the exact locations of the roots.

In our analysis, we are able to characterize the number and locations of unimodular roots of $p(z) = z^n + z^k - 1$ in terms of conditions on n and k.

Necessary and Sufficient Conditions

Let $p(z) = z^n + z^k - 1$ and assume p has a unimodular root $e^{i\theta}$. Substituting $e^{i\theta}$ into the equation $p(z) = 0$ and rearranging gives

$$e^{in\theta} + e^{ik\theta} = 1. \tag{1}$$

The only pair of unimodular complex numbers that sum to 1 are $1/2 \pm i\sqrt{3}/2$. This follows by observing the pair must be conjugates and are constrained to satisfy the equation of the unit circle. In polar form, the numbers $1/2 \pm i\sqrt{3}/2$ can be written as $e^{\pm i\pi/3}$.

Focusing our attention on the angles $n\theta$ and $k\theta$, we see there exists integers α and β satisfying the pair of equations

$$n\theta = \pm\frac{\pi}{3} + 2\pi\alpha \tag{2}$$

$$k\theta = \mp\frac{\pi}{3} + 2\pi\beta. \tag{3}$$

Solving both equations for θ and equating the results gives

$$\pm\frac{\pi}{3n}+\frac{2\pi\alpha}{n}=\mp\frac{\pi}{3k}+\frac{2\pi\beta}{k}.$$

Multiplying through by $3nk/\pi$ and simplifying leads to

$$n+k=\pm 6(n\beta-k\alpha). \tag{4}$$

The preceding discussion establishes the following lemma:

Lemma 1. If $p(z)=z^n+z^k-1$ has unimodular roots, then $n+k=0 \bmod 6$.

The result in Lemma 1 gives a necessary condition on n and k, but the condition is not sufficient. Indeed, the polynomials z^4+z^2-1 and z^9+z^3-1 both satisfy $n+k=0 \bmod 6$, but neither has any unimodular roots. We observe in these two examples that $\gcd(n,\,k)\neq 1$. Making the substiutions $w=z^2$ and $u=z^3$ lead to the associated polyomials w^2+w-1 and u^3+u-1 respectively. Neither of these simpler polynomials have any unimodular roots. This observation motivates the following lemma:

Lemma 2. Let $n,k\in\mathbb{N}$, with $1\leq k\leq n-1$, and let $g=\gcd(n,\,k)$. Then $p(z)=z^n+z^k-1$ has unimodular roots if and only if $q(z)=z^{n/g}+z^{k/g}-1$ has unimodular roots.

Proof. Assume λ is unimodular and that $p(\lambda)=0$. Then λ^g is also unimodular and

$$q(\lambda^g)=(\lambda^g)^{n/g}+(\lambda^g)^{k/g}-1=\lambda^n+\lambda^k-1=p(\lambda)=0.$$

Conversely, assume γ is unimodular and $q(\gamma)=0$. Let ω represent any of the unimodular g^{th} roots of γ; so $\omega^g=\gamma$. Then

$$p(\omega)=(\omega)^n+(\omega)^k-1=(\omega^g)^{n/g}+(\omega^g)^{k/g}-1=q(\gamma)=0.$$

■

Lemma 2 makes it clear that we only need to consider polynomials $p(z)=z^n+z^k-1$ in which n and k are relatively prime. In cases where $\gcd(n,\,k)=g>1$, we instead consider the polynomial $q(z)=z^{n/g}+z^{k/g}-1$. The unimodular roots of p are in g-to-1 correspondence with the unimodular roots of q.

With the restriction $\gcd(n,\,k)=1$, we can state and prove the converse to Lemma 1. The proof will depend on the following classical result from the theory of linear Diophantine equations (see [1], pg. 35 for a complete discussion).

Theorem 1. *The integer equation $ax+by=c$ has a solution if and only if g divides c, where $g=\gcd(a,\,b)$. Moreover, if $x=x_0$ and $y=y_0$ is one particular solution, then the complete integer solution is given by*

$$x=x_0+m\frac{b}{g}\qquad y=y_0-m\frac{a}{g},$$

where $m\in\mathbb{Z}$.

Lemma 3. If $n+k=0 \bmod 6$ and $\gcd(n,\,k)=1$, then $e^{\pm i\pi/3}$ are the only unimodular roots of $p(z)=z^n+z^k-1$.

Proof. The hypotheses on n and k imply that neither is divisible by 2 or 3 (exercise). Thus both integers are of the form $\pm 1 \bmod 6$. Hence, there exist non-negative integers s and t such that $n = 6s \pm 1$ and $k = 6t \mp 1$.

We assume $n = 6s + 1$ and $k = 6t - 1$, with the other case being very similar. Thus, we can write

$$p(z) = z^{6s+1} + z^{6t-1} - 1 = z^{6s}z + z^{6t}\left(\frac{1}{z}\right) - 1.$$

A direct calculation shows $p\left(e^{\pm i\pi/3}\right) = 0$.

Now assume $p(e^{i\theta}) = 0$. We will show that $\theta = \pm\frac{\pi}{3}$ up to addition by a multiple of 2π. We note that equation (4) was derived under the assumption that p had a unimodular root. Equation (4) is really two linear diophantine equations in the variables α and β :

$$-6k\alpha + 6n\beta = n + k \tag{5}$$

$$6k\alpha - 6n\beta = n + k. \tag{6}$$

To see that Theorem 1 applies we need $\gcd(6k,\ 6n)$ to divide $n + k$. It readily follows from $\gcd(n,\ k) = 1$ that $\gcd(6k,\ 6n) = 6$, and we assumed $n + k$ is divisible by 6.

Recalling that $n = 6s + 1$ and $k = 6t - 1$, we leave it as an exercise for the reader to verify that the pair $\alpha = s,\ \beta = t$ is a solution to equation (5), and the pair $\alpha = n - s,\ \beta = k - t$ is a solution to equation (6). Thus, by Theorem 1, the complete set of integer solutions to equation (5) is given by

$$\alpha = s + m \cdot n \qquad \beta = t + m \cdot k, \tag{7}$$

where $m \in \mathbb{Z}$. Similarly, the complete set of integer solutions to equation (6) is given by

$$\alpha = n - s - m \cdot n \qquad \beta = k - t - m \cdot k, \tag{8}$$

where $m \in \mathbb{Z}$.

Now, adding equations (2) and (3), making the substitutions $n = 6s + 1$ and $k = 6t - 1$, and solving for θ yields

$$\theta = \frac{\pi}{3} \cdot \frac{\alpha + \beta}{s + t}. \tag{9}$$

Substituting the possible values for α and β from (7) and (8) into equation (9) gives $\theta = \pm\frac{\pi}{3} \bmod 2\pi$ as required. ∎

The Complete Result

We can now completely characterize when and where the unimodular roots occur for our family of polynomials.

Theorem 2. *Let $p(z) = z^n + z^k - 1$ and let $g = \gcd(n,\ k)$. If 6 divides $n/g + k/g$, then p has exactly $2g$ unimodular roots, z_m and $\bar{z}_m$, given by*

$$z_m = \exp\left[i\left(\frac{\pi}{3g} + \frac{2\pi m}{g}\right)\right],$$

where $0 \leq m \leq g - 1$.

As an illustration of the theorem, suppose that $n = 70$. By trial and error we see that there are only six values of k satisfying

$$\frac{70}{\gcd(70, k)} + \frac{k}{\gcd(70, k)} = 0 \bmod 6.$$

These values and the number of unimodular roots are shown in Table 1.

k	$\gcd(70, k)$	Number of unimodular roots
2	2	4
14	14	28
26	2	4
38	2	4
50	10	20
62	2	4

Table 1. For $n = 70$, the values of k resulting in unimodular roots.

In the preceding example, there were six k-values for which the resulting polynomial had unimodular roots. There are 64 unimodular roots out of 4830 total roots for the entire family $p(z) = z^{70} + z^k - 1$. The number of unimodular roots for a family varies widely with the value of n. In constrast to the case where $n = 70$, there are arbitrarily large values of n such that for all $1 \leq k \leq n - 1$ there are no unimodular roots; any $n = 2^\mu \cdot 3^\nu$, where $\mu, \nu \in \mathbb{N}$ is an example.

The case where $n \geq 5$ is prime is more tractable. Here, the hypotheses of Theorem 2 are satisfied by the smallest integer k_0 for which $n + k_0$ is a multiple of 6. Starting from k_0, there are also unimodular roots for $k = k_0 + 6m$, $m = 0, 1, \ldots$, as long as $k \leq n - 1$. In each such case, there will be exactly one pair of conjugate unimodular roots.

Finally, the requirement that $n + k = 0 \bmod 6$, with $\gcd(n, k) = 1$ implies that $n = 5$ and $k = 1$ are the smallest possible values of n and k that result in unimodular roots.

Problems for Investigation

We conclude this paper by describing possible areas for further research. Some of these questions may be suitable for advanced undergraduate projects.

1. For fixed n, what is the total number of unimodular roots for the family of polynomials $p(z) = z^n + z^k - 1$, where $1 \leq k \leq n - 1$? It is straightforward to answer this question when n is prime. However, as shown in the example above with $n = 70$, it is more difficult when n is composite.
2. An obvious extension of our problem is to insert two lower order terms. Thus, consider the family of polynomials given by $p(z) = z^n + z^k + z^j - 1$, where $1 \leq j < k \leq n - 1$. Special cases such as $j = k - 1$ and $j = n - k$ might good places to start.
3. For all pairs n and k, we observed that roots occur both inside and outside the unit circle. It is a straightforward application of Rouche's theorem (see [4]) to determine an annular band about C in which all the roots must lie, and to see that the band

gets narrower with increasing values of n. Fixing n and allowing k to vary, numerical experiments show complicated patterns for the number of roots inside or outside the unit circle. However, if one views half of the unimodular roots as occuring inside and half outside the unit circle, then more predictable patterns occur. Restricting to the case where n is prime and letting k increase, we find the number of roots inside or outside the unit circle as a function of k only changes when $n + k = 0 \bmod 6$.

4. As seen in Figure 3, the set of roots from the family of polynomials $p(z) = z^n + z^k - 1$ (with n fixed) presents a striking image. It is interesting to animate this process by plotting the complete set of roots for each value of k, as k increases from 1 to $n - 1$. The animation shows that the roots appear to loop around the n^{th} roots of unity at different rates. We are happy to provide our *Mathematica* code showing these animations to any interested reader.

Summary.

We investigate the family of polynomials $p(z) = z^n + z^k - 1$ and characterize the number and location of unimodular roots in terms of conditions on n and k. The main result shows that unimodular roots occur if and only if $n/g + k/g$ is divisible by 6, where $g = \gcd(n, k)$. In this case, there are exactly g pairs of conjugate unimodular roots.

References

1. W. J. Gilbert and S. A. Vanstone, *An Introduction to Mathematical Thinking: Algebra and Number Systems* Pearson Prentice Hall, Upper Saddle River, NJ, 2005.
2. A. Melman, Geometry of Trinomials, *Pacific Journal of Mathematics* **259, No. 1** (2012) 141-159.
3. P. Stocia and R. Moses, On the Unit Circle Problem: The Schur-Cohn Procedure Revisited, *Signal Processing* **26** (1992) 95-118.
4. D. G. Zill and P. D. Shanahan, *A First Course In Complex Analysis,* Jones and Bartlett, Boston-Toronto-London-Singapore, 2009.